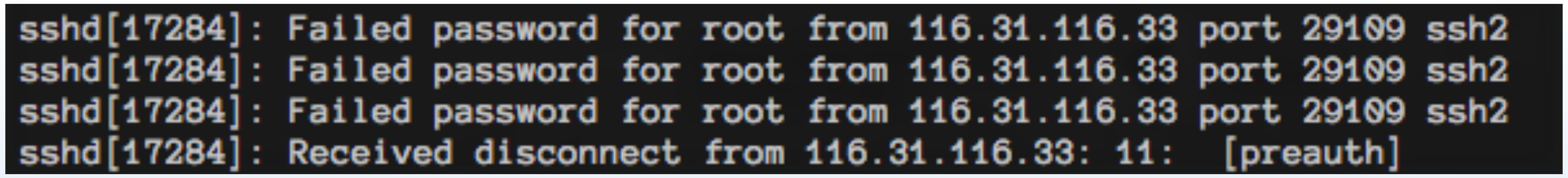
The Naughty Step

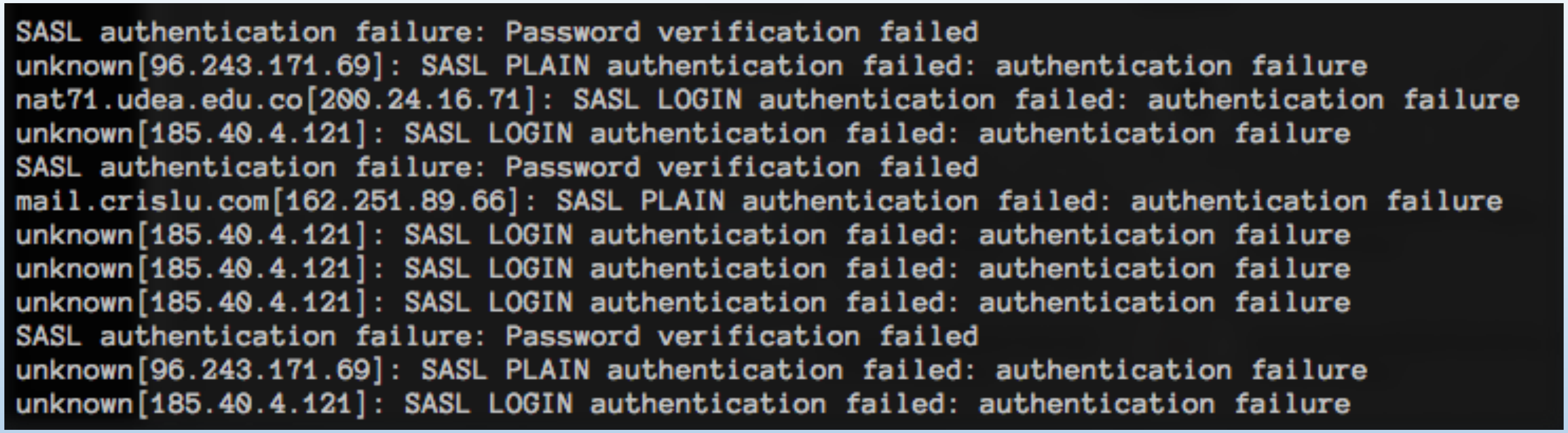
Marek Isalski — @maznu
Faelix Limited — https://faelix.net/



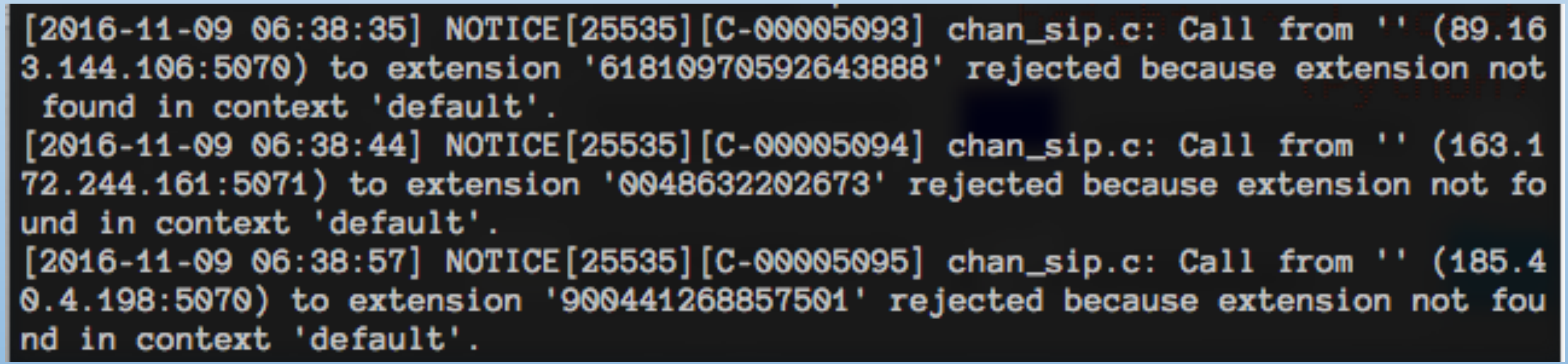
```
sshd[17284]: Failed password for root from 116.31.116.33 port 29109 ssh2
sshd[17284]: Failed password for root from 116.31.116.33 port 29109 ssh2
sshd[17284]: Failed password for root from 116.31.116.33 port 29109 ssh2
sshd[17284]: Received disconnect from 116.31.116.33: 11:  [preauth]
```

ssh

SMTP
IMAP
POP



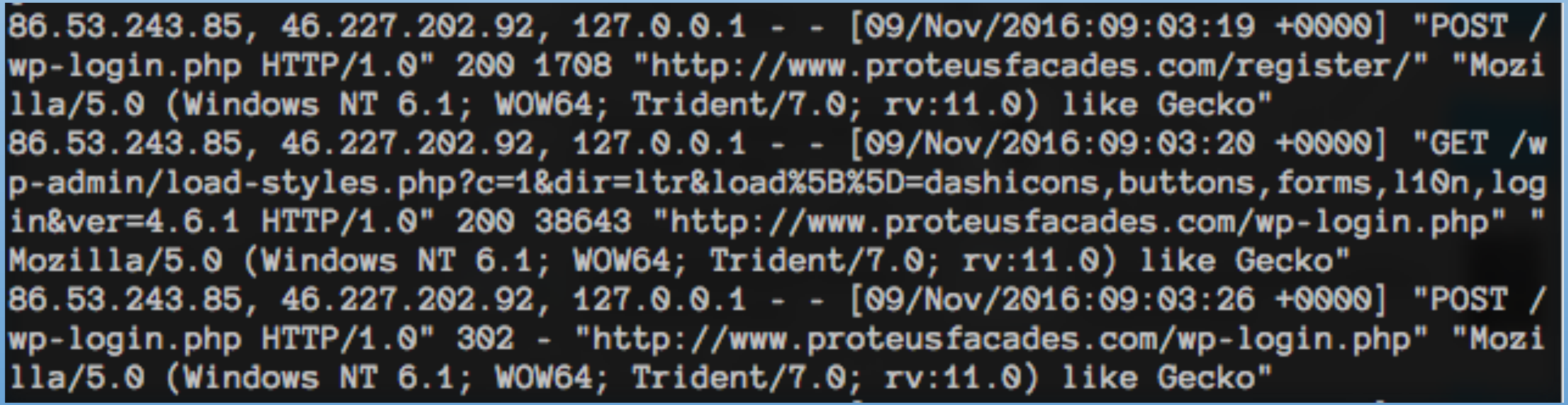
```
SASL authentication failure: Password verification failed
unknown[96.243.171.69]: SASL PLAIN authentication failed: authentication failure
nat71.udea.edu.co[200.24.16.71]: SASL LOGIN authentication failed: authentication failure
unknown[185.40.4.121]: SASL LOGIN authentication failed: authentication failure
SASL authentication failure: Password verification failed
mail.crislu.com[162.251.89.66]: SASL PLAIN authentication failed: authentication failure
unknown[185.40.4.121]: SASL LOGIN authentication failed: authentication failure
unknown[185.40.4.121]: SASL LOGIN authentication failed: authentication failure
unknown[185.40.4.121]: SASL LOGIN authentication failed: authentication failure
SASL authentication failure: Password verification failed
unknown[96.243.171.69]: SASL PLAIN authentication failed: authentication failure
unknown[185.40.4.121]: SASL LOGIN authentication failed: authentication failure
```



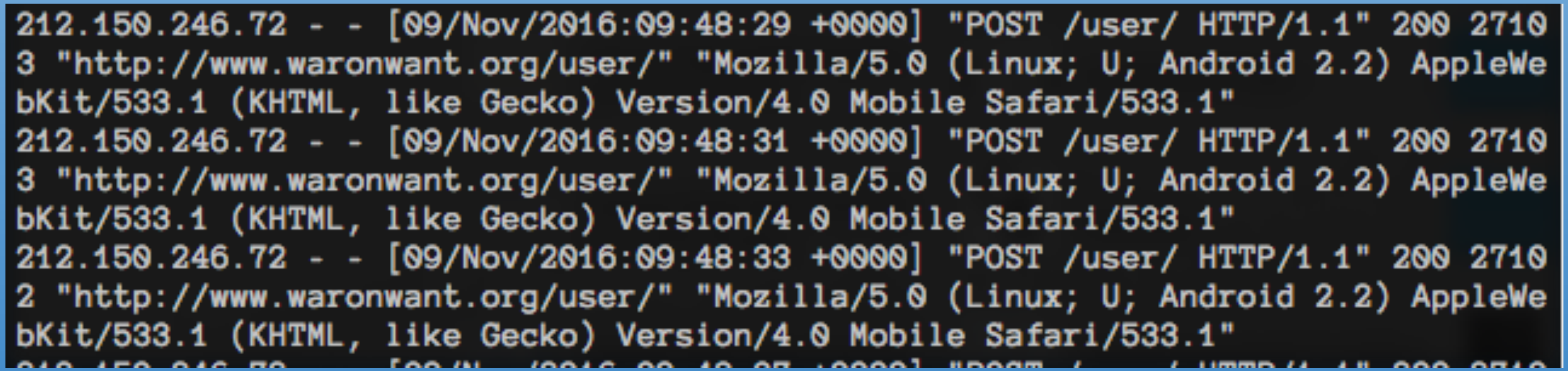
```
[2016-11-09 06:38:35] NOTICE[25535][C-00005093] chan_sip.c: Call from '' (89.16
3.144.106:5070) to extension '618109705926438888' rejected because extension not
 found in context 'default'.
[2016-11-09 06:38:44] NOTICE[25535][C-00005094] chan_sip.c: Call from '' (163.1
72.244.161:5071) to extension '0048632202673' rejected because extension not fo
und in context 'default'.
[2016-11-09 06:38:57] NOTICE[25535][C-00005095] chan_sip.c: Call from '' (185.4
0.4.198:5070) to extension '900441268857501' rejected because extension not fou
nd in context 'default'.
```

VOIP

WordPress



```
86.53.243.85, 46.227.202.92, 127.0.0.1 - - [09/Nov/2016:09:03:19 +0000] "POST /
wp-login.php HTTP/1.0" 200 1708 "http://www.proteusfacades.com/register/" "Mozi
lla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
86.53.243.85, 46.227.202.92, 127.0.0.1 - - [09/Nov/2016:09:03:20 +0000] "GET /w
p-admin/load-styles.php?c=1&dir=ltr&load%5B%5D=dashicons,buttons,forms,l10n,log
in&ver=4.6.1 HTTP/1.0" 200 38643 "http://www.proteusfacades.com/wp-login.php" "
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
86.53.243.85, 46.227.202.92, 127.0.0.1 - - [09/Nov/2016:09:03:26 +0000] "POST /
wp-login.php HTTP/1.0" 302 - "http://www.proteusfacades.com/wp-login.php" "Mozi
lla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
```



```
212.150.246.72 - - [09/Nov/2016:09:48:29 +0000] "POST /user/ HTTP/1.1" 200 2710
3 "http://www.waronwant.org/user/" "Mozilla/5.0 (Linux; U; Android 2.2) AppleWe
bKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1"
212.150.246.72 - - [09/Nov/2016:09:48:31 +0000] "POST /user/ HTTP/1.1" 200 2710
3 "http://www.waronwant.org/user/" "Mozilla/5.0 (Linux; U; Android 2.2) AppleWe
bKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1"
212.150.246.72 - - [09/Nov/2016:09:48:33 +0000] "POST /user/ HTTP/1.1" 200 2710
2 "http://www.waronwant.org/user/" "Mozilla/5.0 (Linux; U; Android 2.2) AppleWe
bKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1"
```

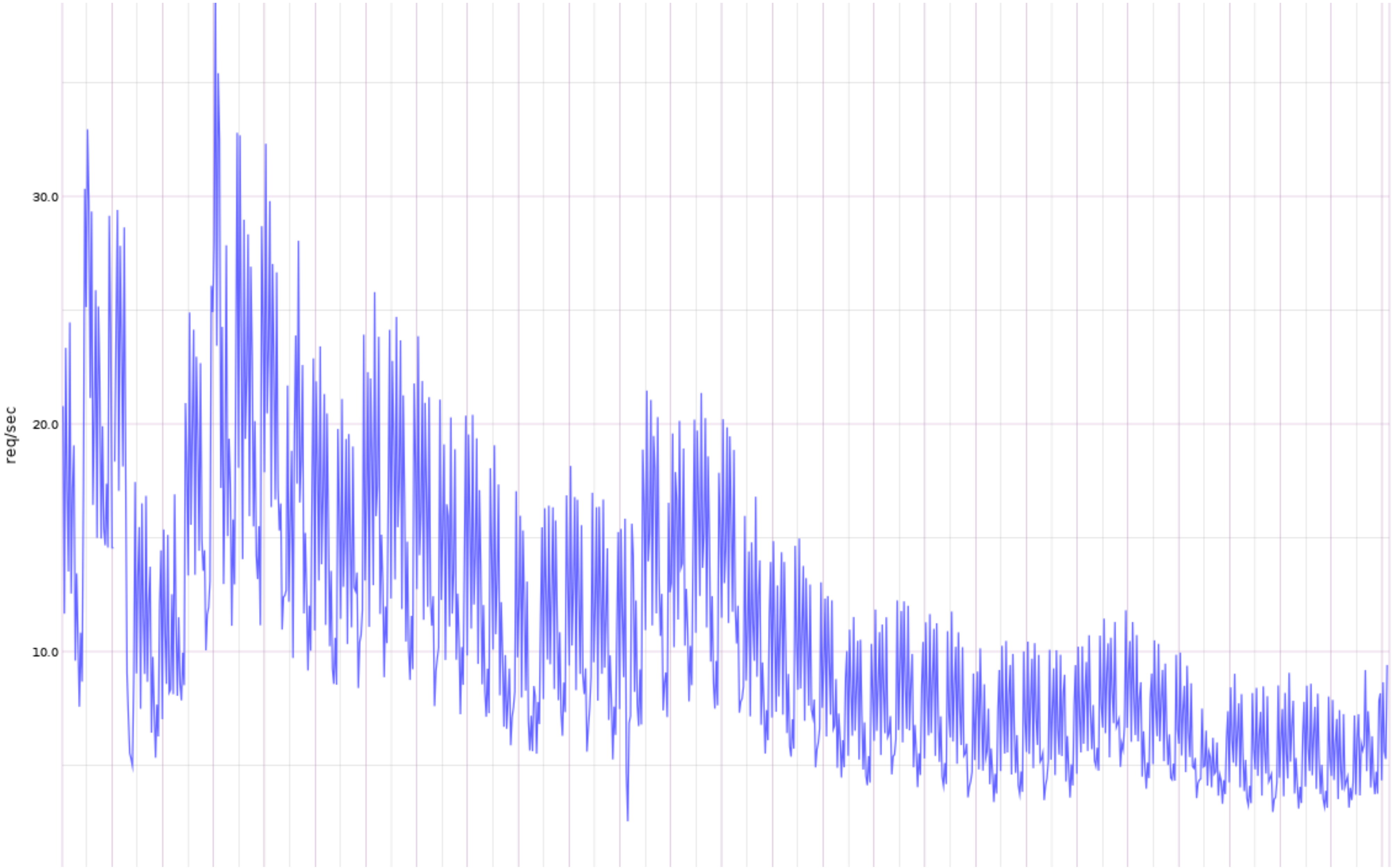
Drupal

That is one big pile of shit!
MOVIECLIPS.COM

The Naughty Step

The Shit Pit

~~The Naughty Step~~



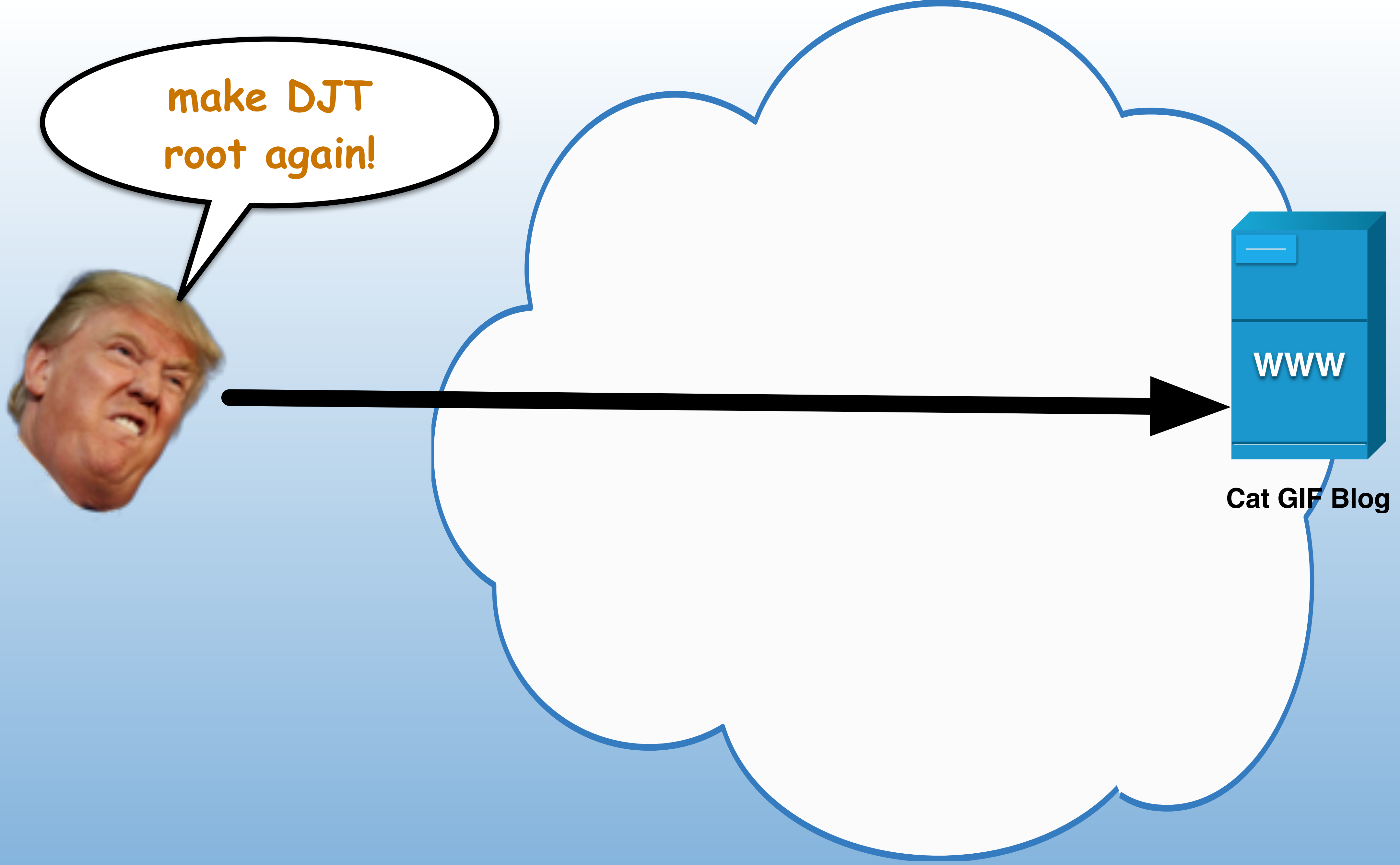
PushDo

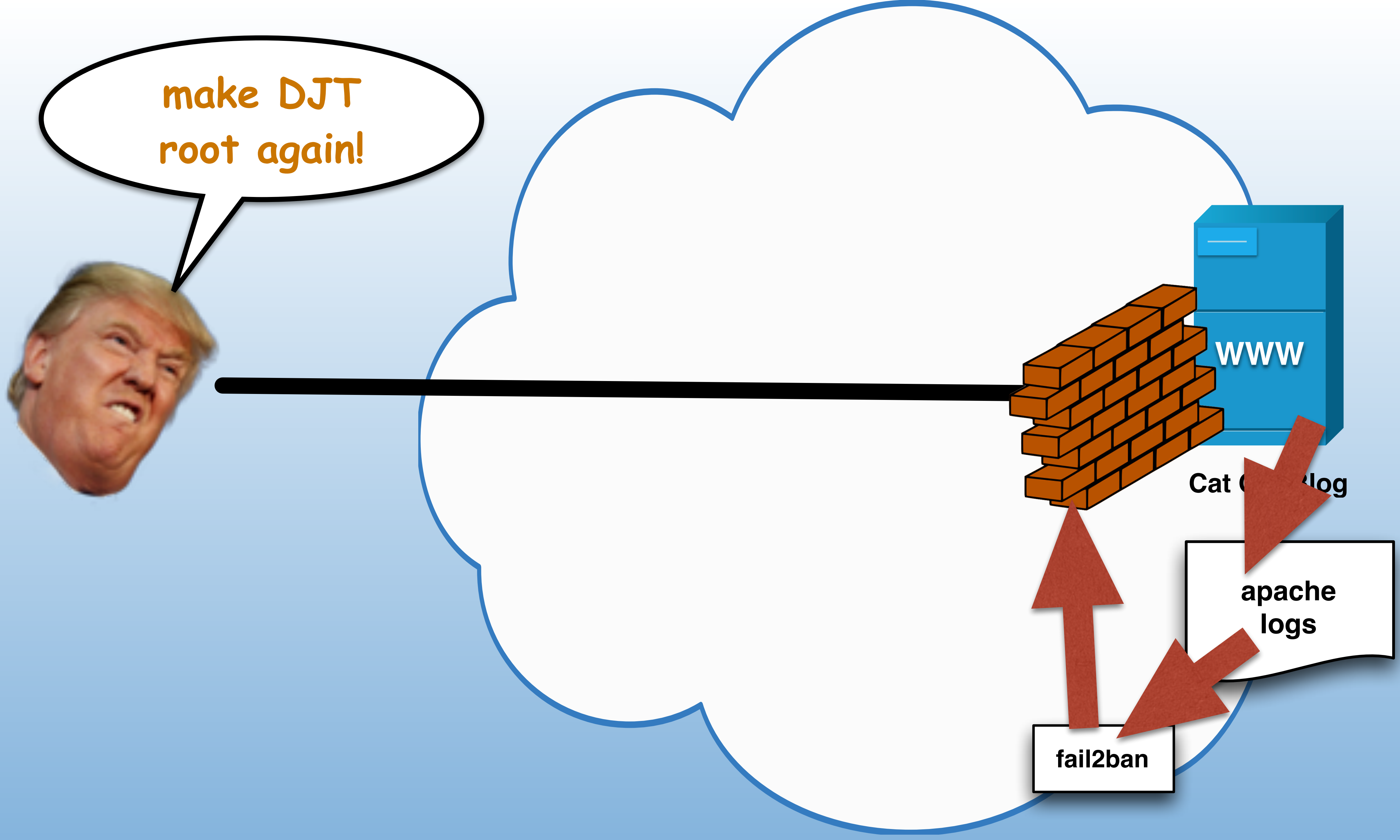
virus cover traffic sending 2kbytes with POST / HTTP/1.0
and opening connection to TCP port 25

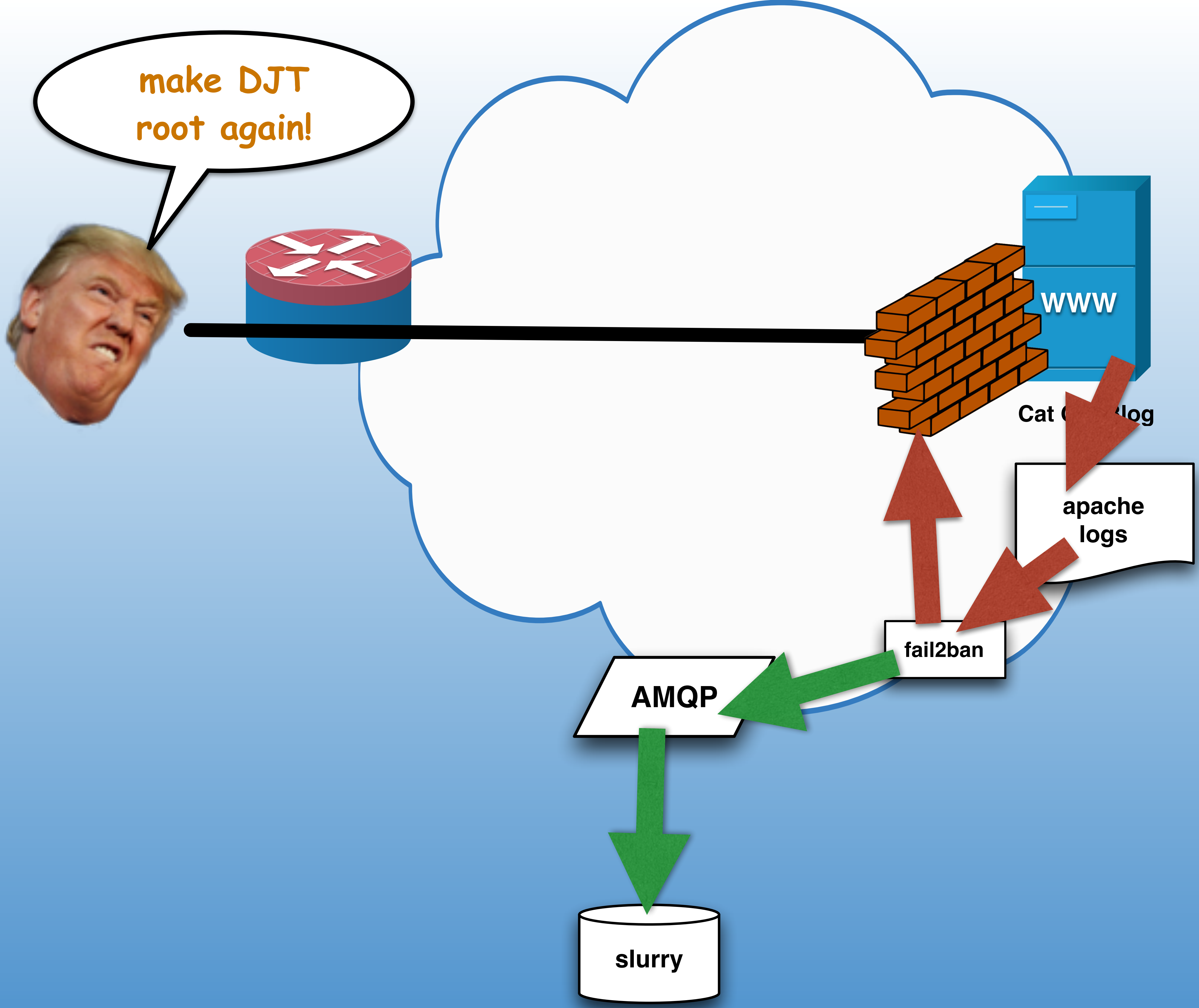
omg wtf loadavg

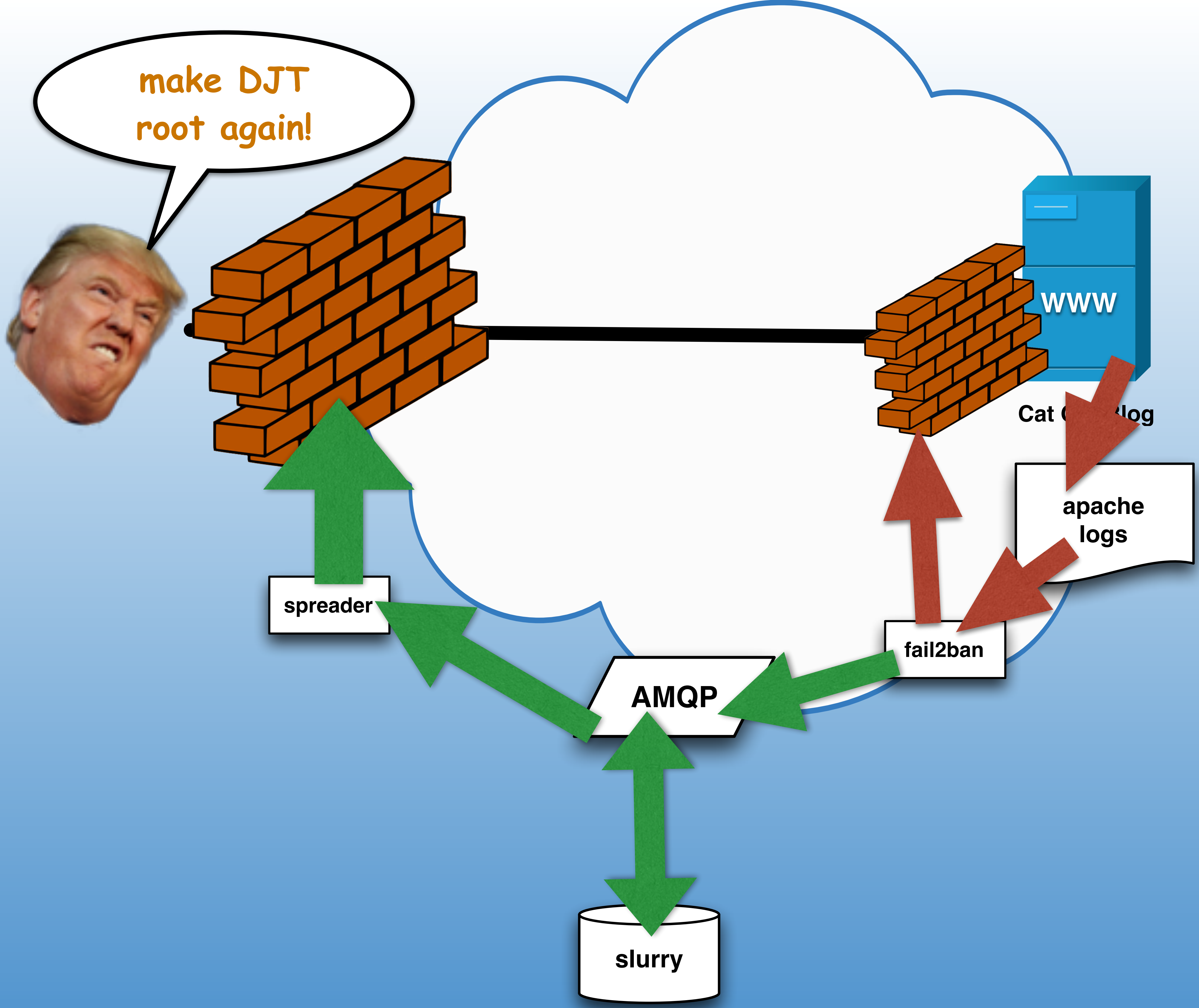
“Security is hard.”

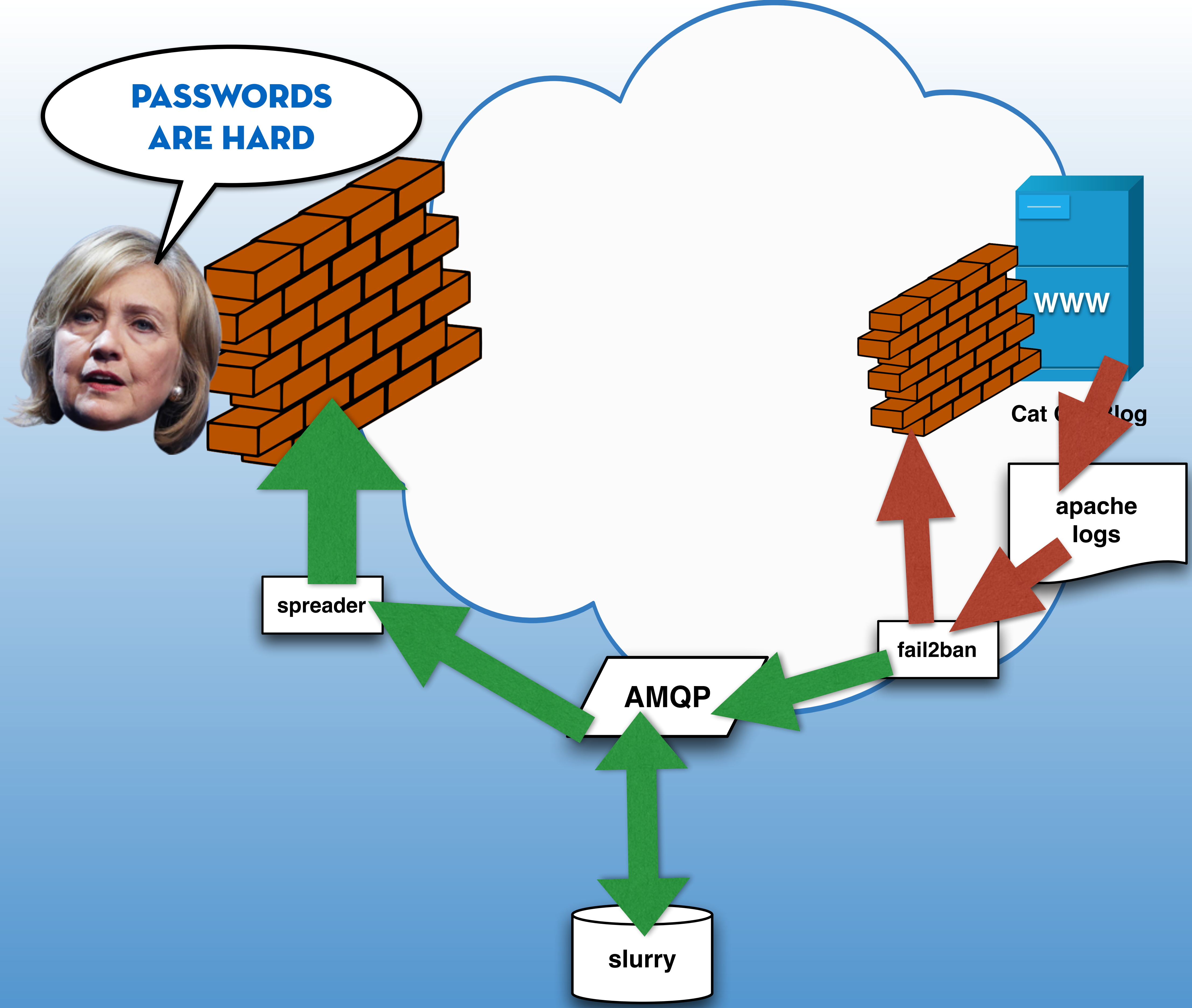
– every infosec professional ever


make DJT root again!
WWW
Cat GIF Blog


make DJT root again!
www
Cat C log
apache logs
fail2ban


make DJT
root again!
WWW
Cat C log
apache logs
fail2ban
AMQP
slurry


make DJT
root again!
www
Cat C [illegible] Blog
apache logs
spreader
fail2ban
AMQP
slurry



WWW

Cat C[illegible] Blog

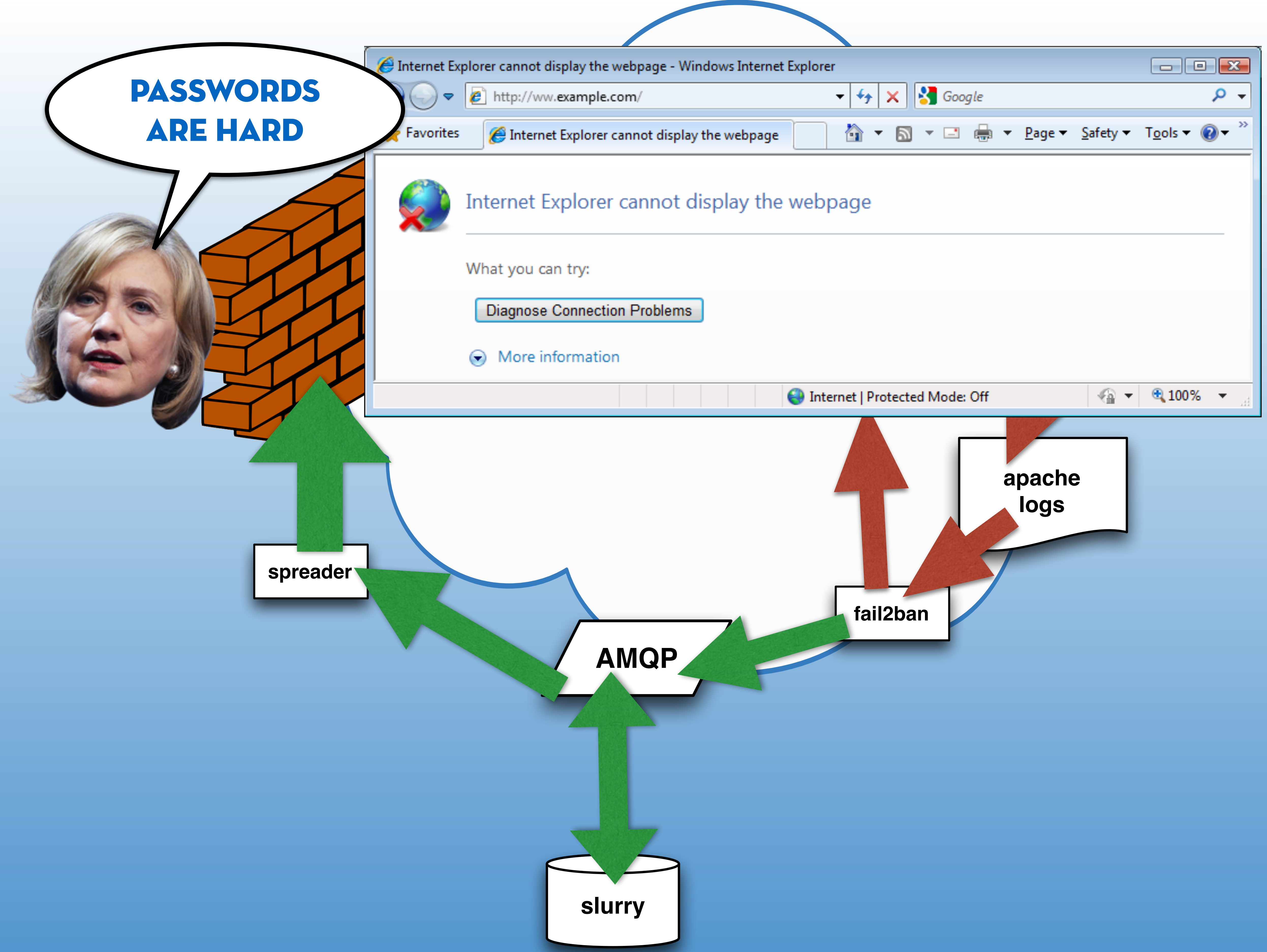
apache
logs

fail2ban

spreader

AMQP

slurry



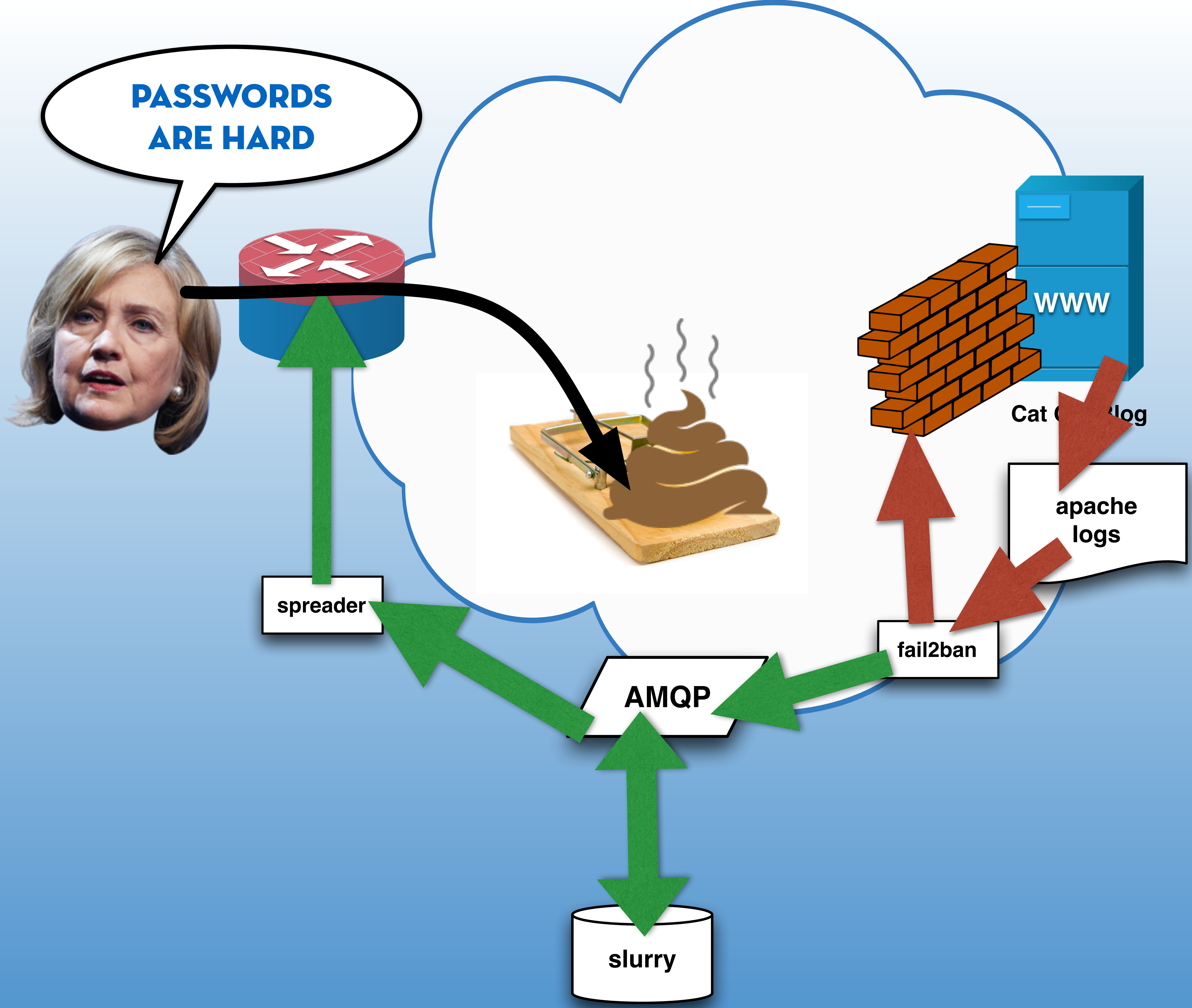
PASSWORDS ARE HARD
Internet Explorer cannot display the webpage - Windows Internet Explorer
http://ww.example.com/
Google
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet | Protected Mode: Off
100%
spreader
AMQP
slurry
fail2ban
apache logs

Internet Explorer cannot display the webpage

What you can try:

Diagnose Connection Problems

More information


PASSWORDS ARE HARD

WWW

Cat C log

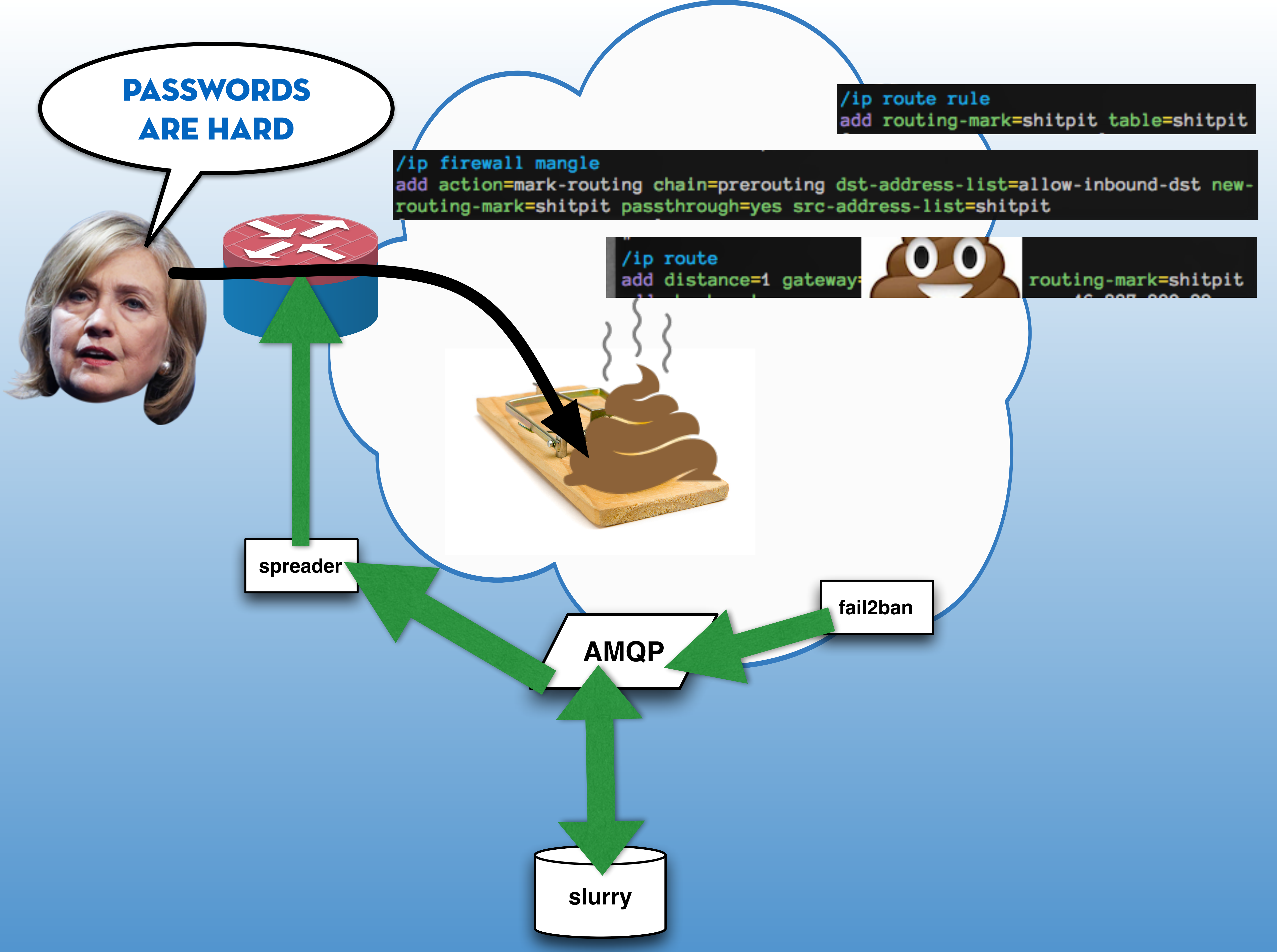
apache logs

fail2ban

AMQP

spreader

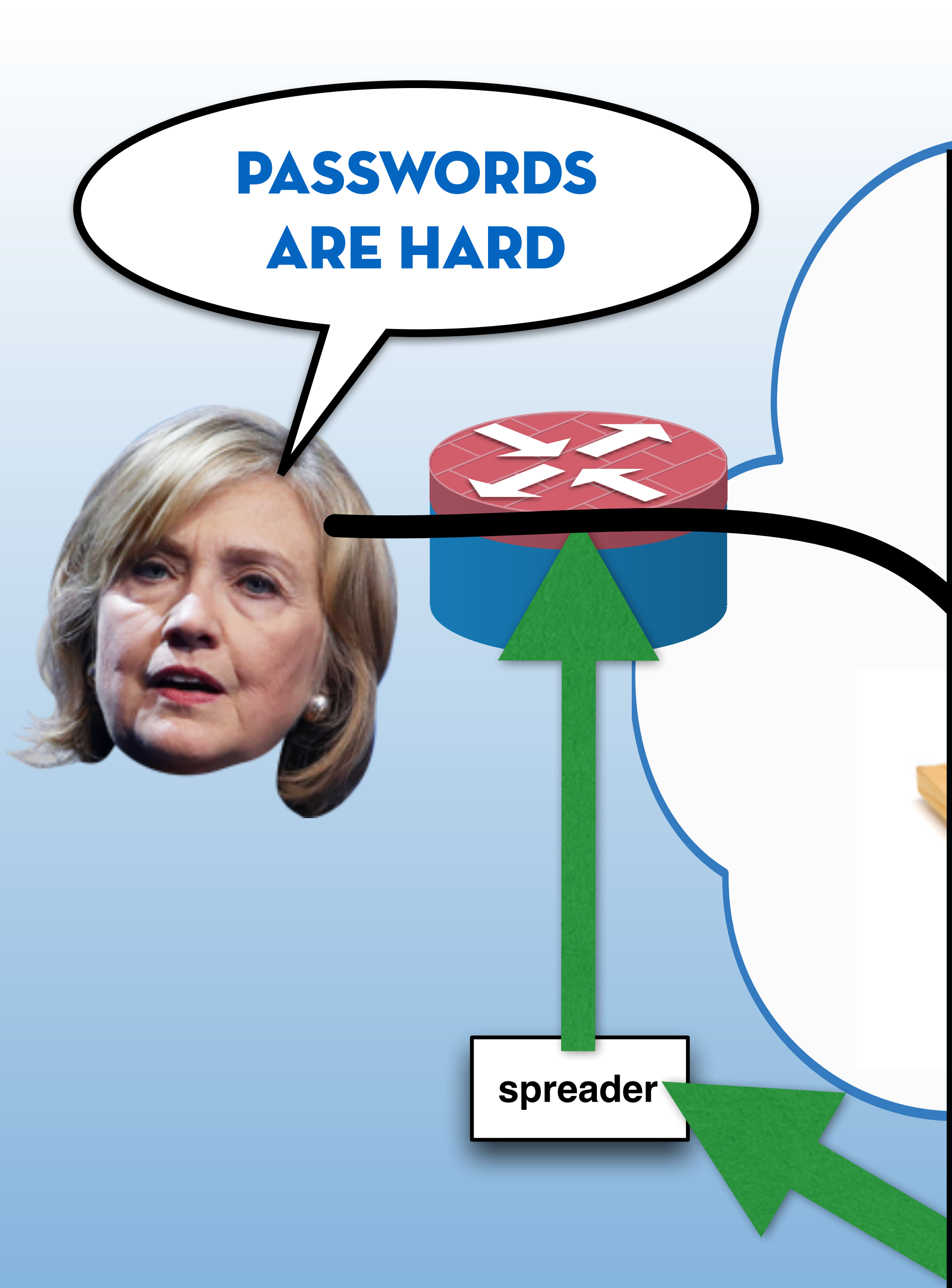
slurry

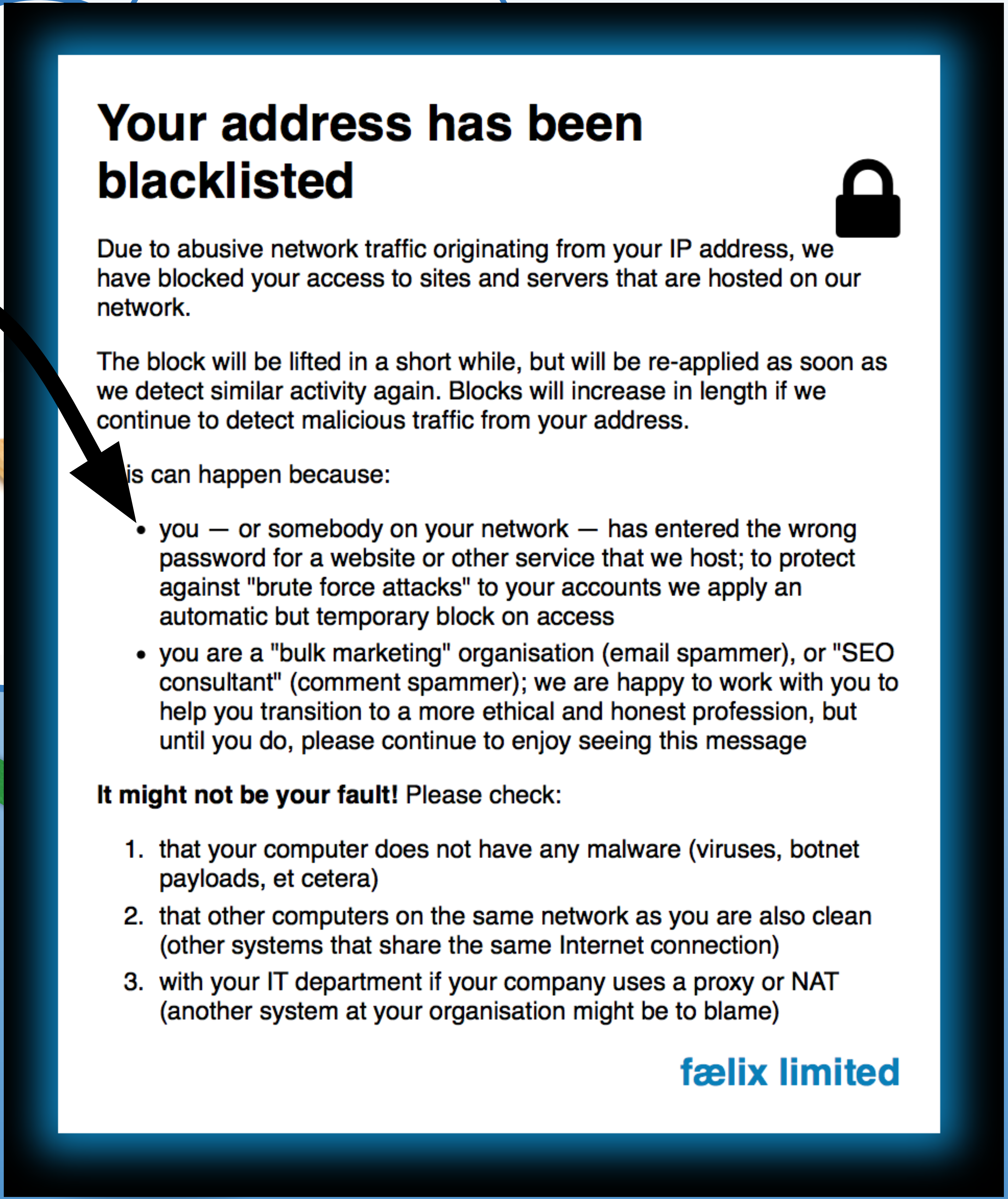


```
/ip route rule
add routing-mark=shitpit table=shitpit
```

```
/ip firewall mangle
add action=mark-routing chain=prerouting dst-address-list=allow-inbound-dst new-routing-mark=shitpit passthrough=yes src-address-list=shitpit
```

```
/ip route
add distance=1 gateway=[redacted] routing-mark=shitpit
```





Your address has been blacklisted

Due to abusive network traffic originating from your IP address, we have blocked your access to sites and servers that are hosted on our network.

The block will be lifted in a short while, but will be re-applied as soon as we detect similar activity again. Blocks will increase in length if we continue to detect malicious traffic from your address.

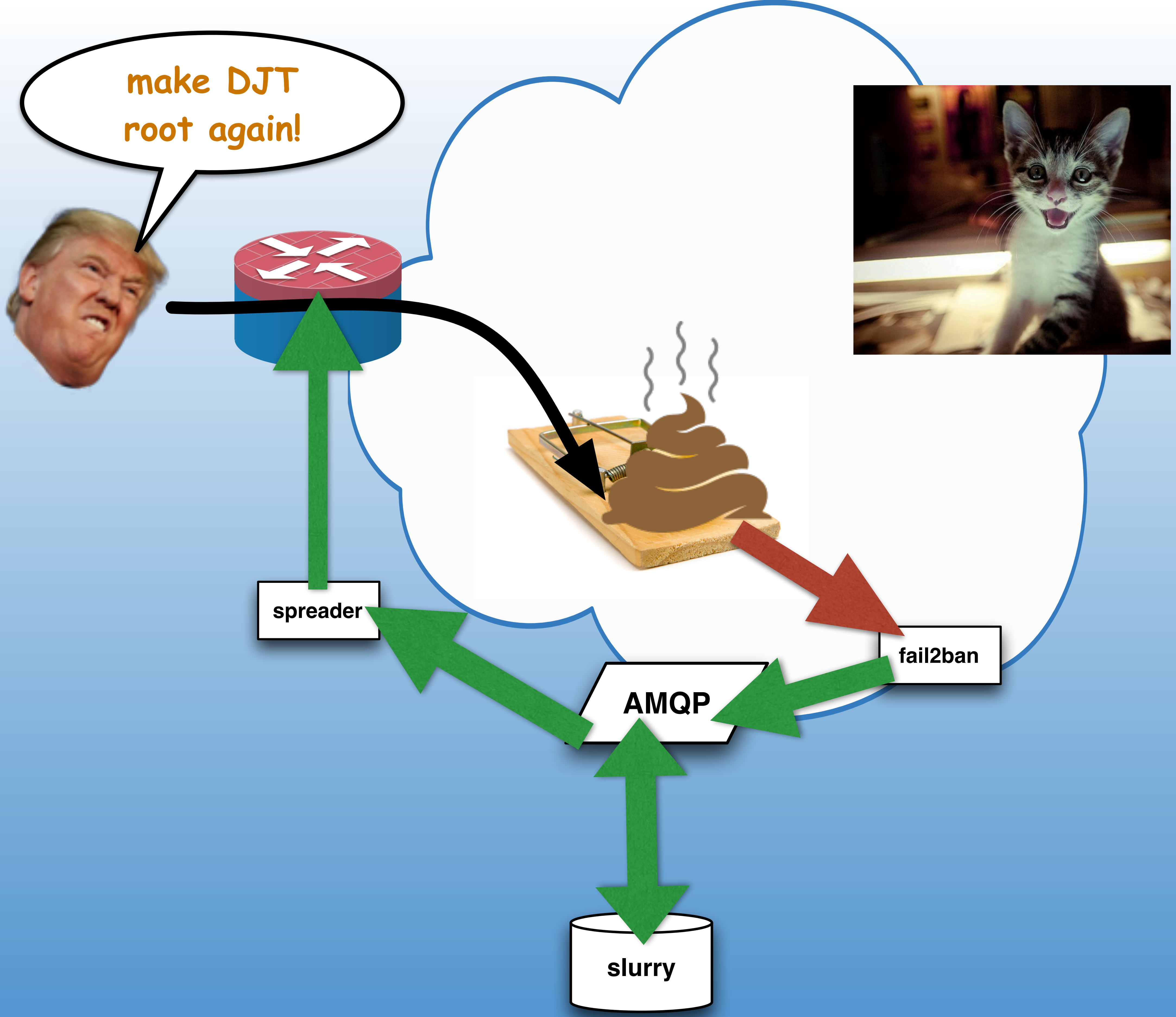
is can happen because:

- you — or somebody on your network — has entered the wrong password for a website or other service that we host; to protect against "brute force attacks" to your accounts we apply an automatic but temporary block on access
- you are a "bulk marketing" organisation (email spammer), or "SEO consultant" (comment spammer); we are happy to work with you to help you transition to a more ethical and honest profession, but until you do, please continue to enjoy seeing this message

It might not be your fault! Please check:

1. that your computer does not have any malware (viruses, botnet payloads, et cetera)
2. that other computers on the same network as you are also clean (other systems that share the same Internet connection)
3. with your IT department if your company uses a proxy or NAT (another system at your organisation might be to blame)

fælix limited

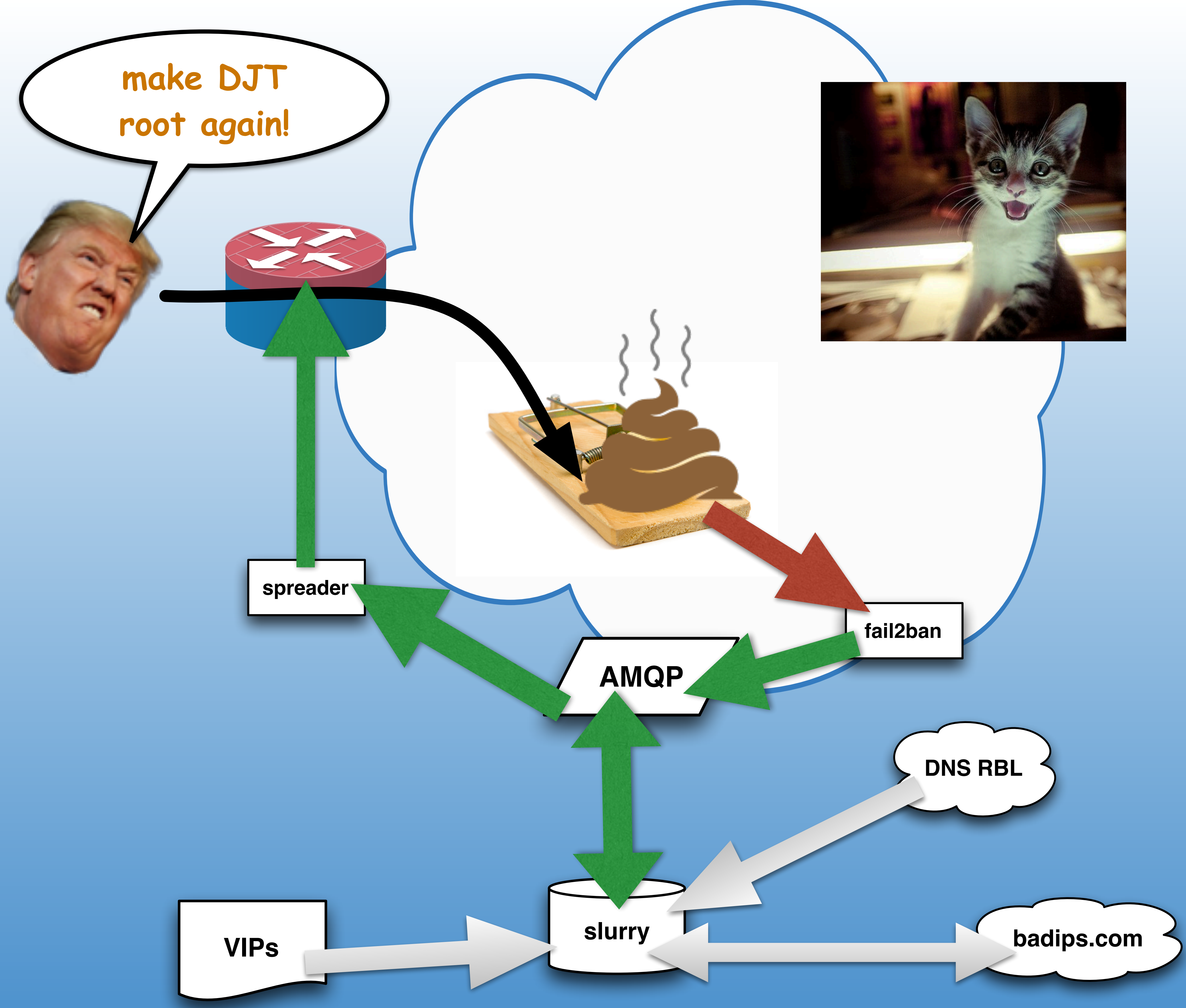


spreader

AMQP

fail2ban

slurry



spreader

fail2ban

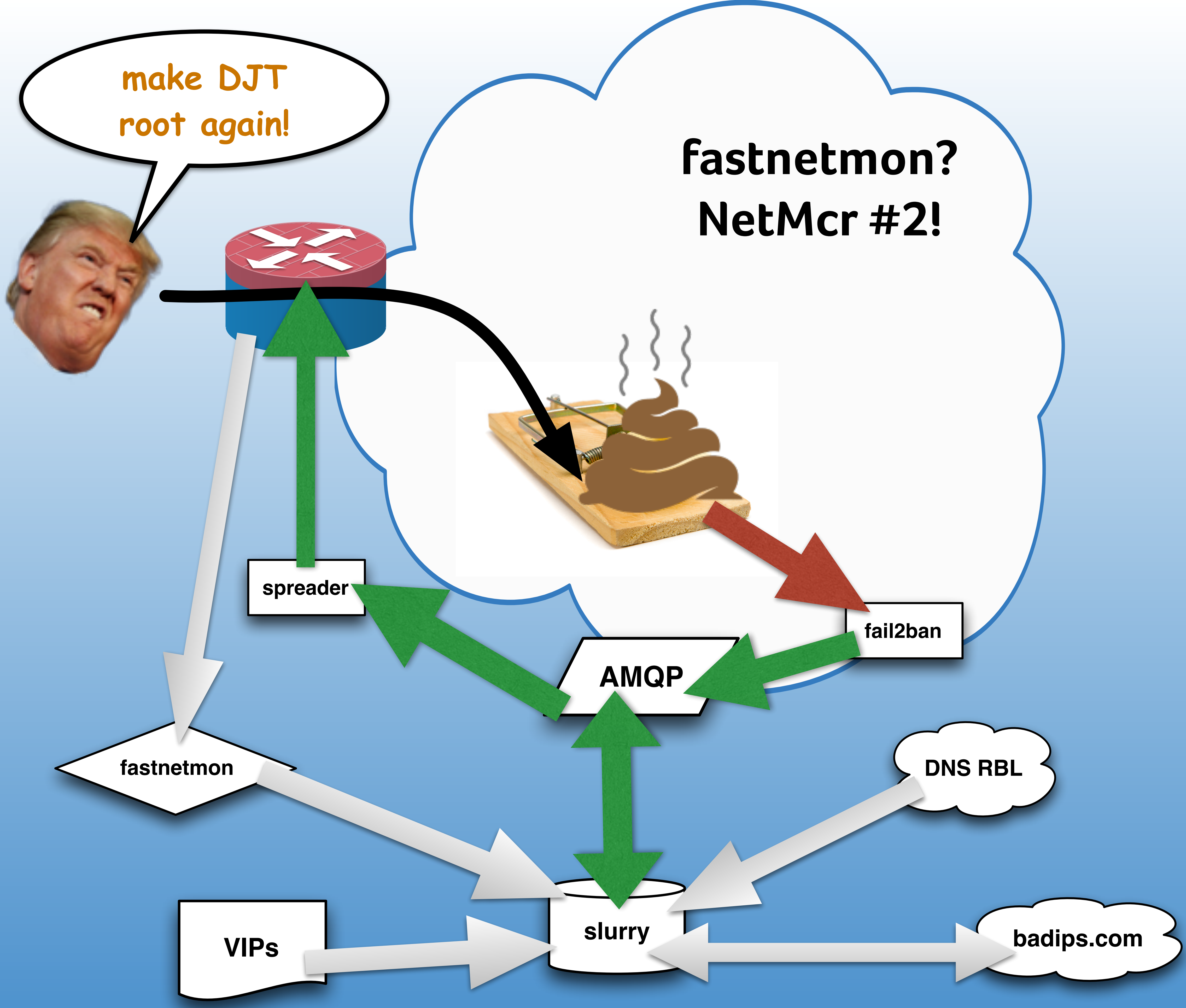
AMQP

DNS RBL

VIPs

slurry

badips.com



fastnetmon?
NetMcr #2!

spreader

fail2ban

AMQP

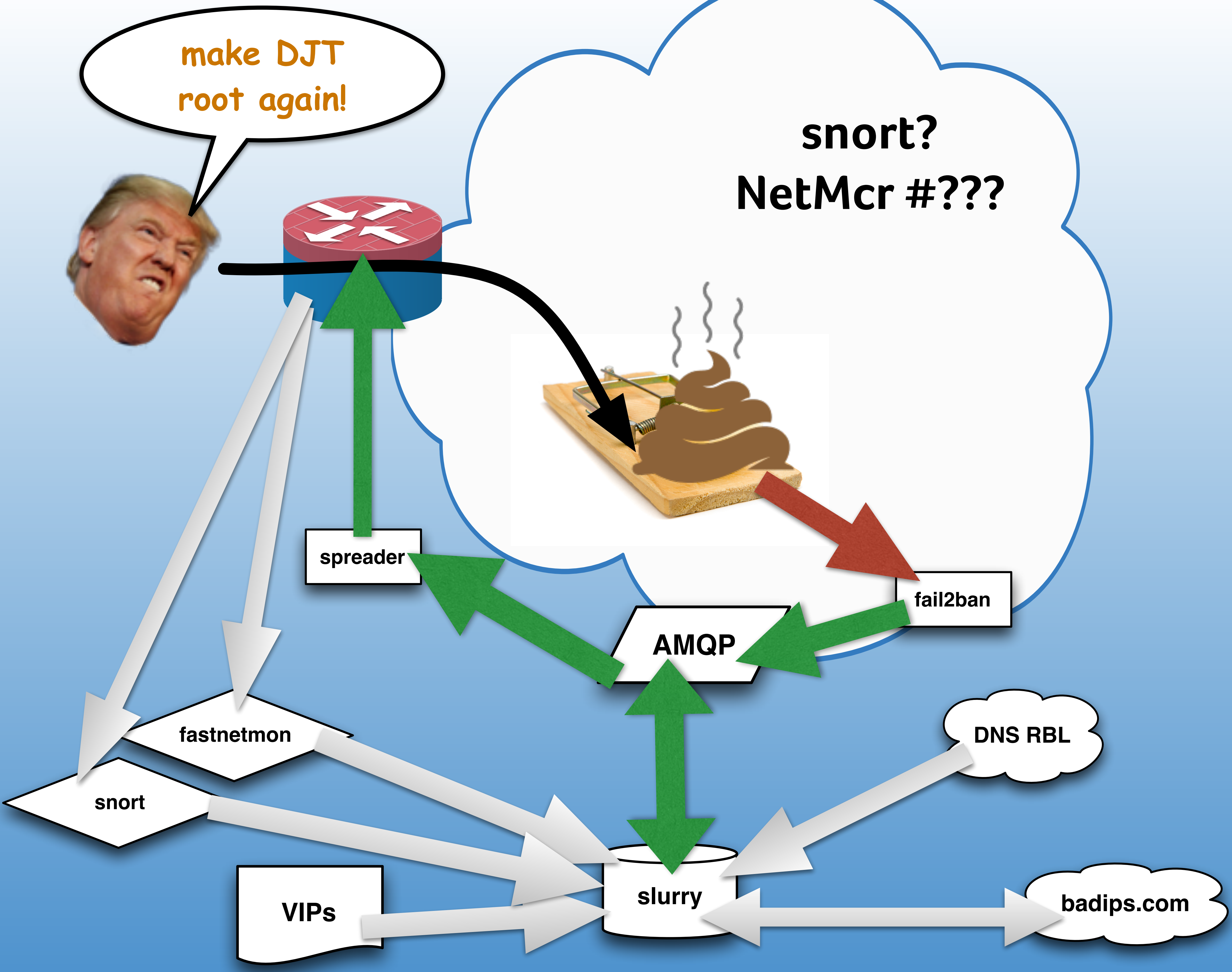
fastnetmon

DNS RBL

slurry

VIPs

badips.com



snort?

NetMcr #???

spreader

fail2ban

AMQP

fastnetmon

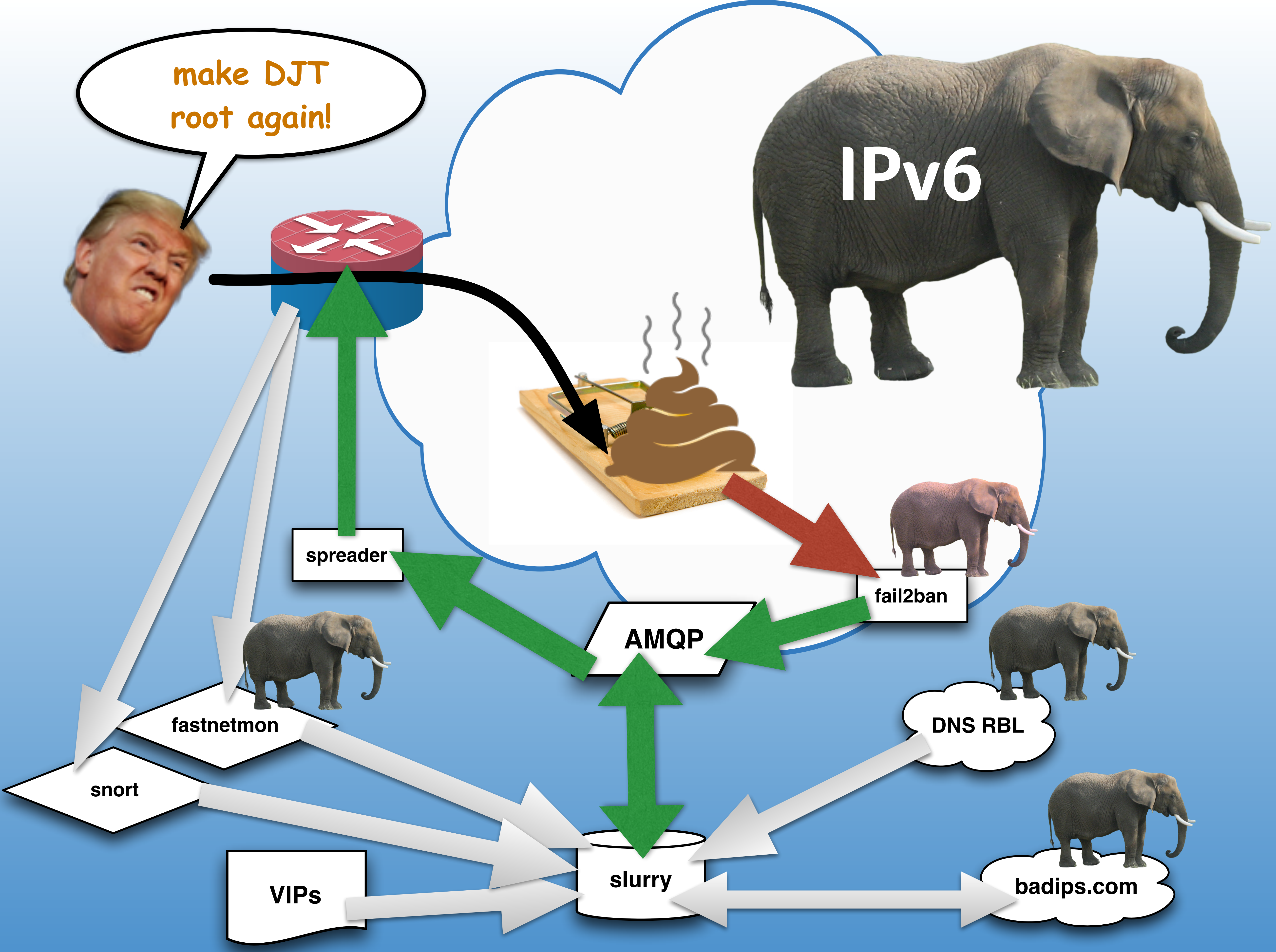
snort

DNS RBL

slurry

VIPs

badips.com



spreader

fail2ban

AMQP

fastnetmon

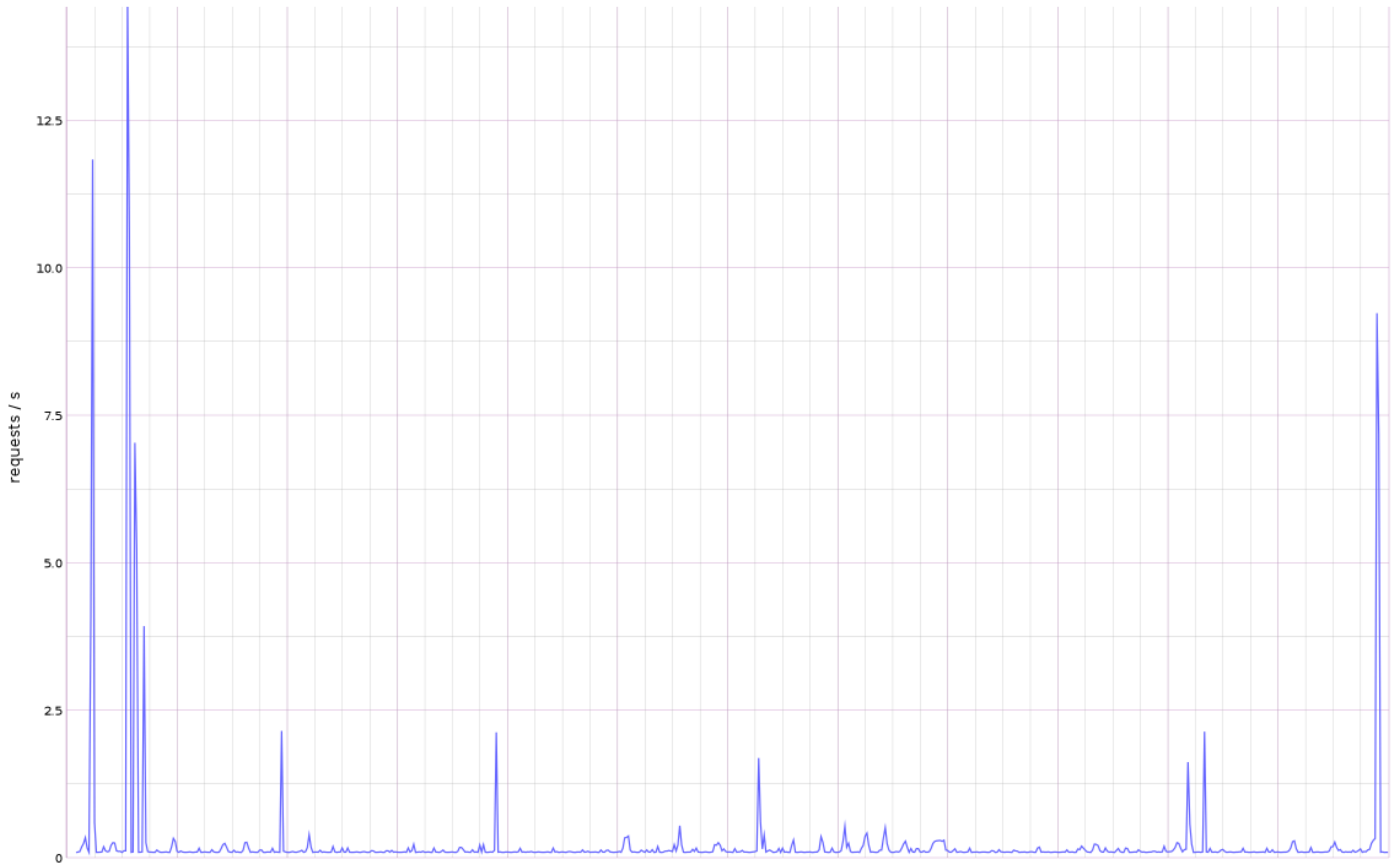
snort

DNS RBL

slurry

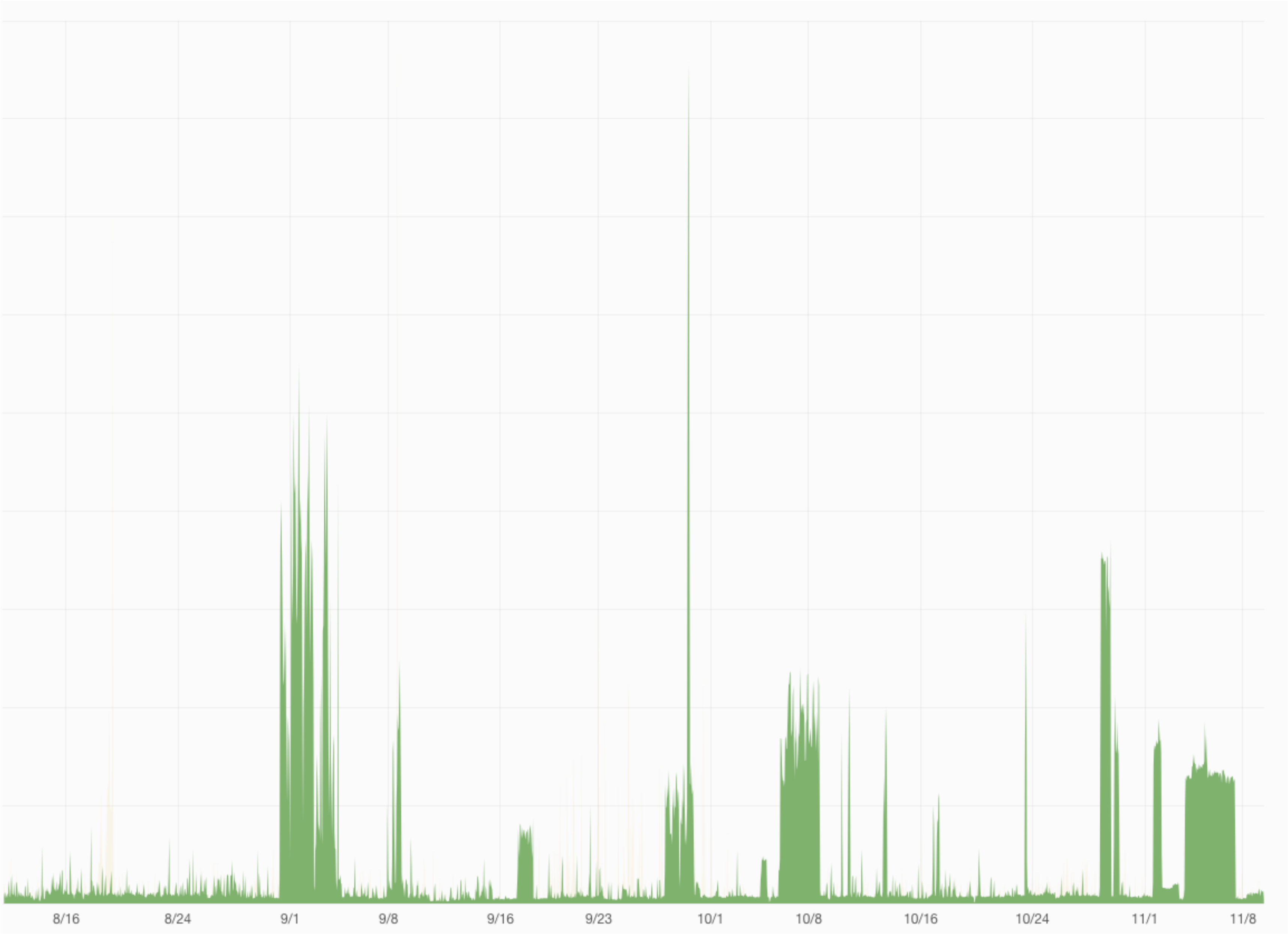
VIPs

badips.com



bots = smart

Typical day of traffic in the shitpit:
spike of traffic, bot realises, moves on.



bots = dumb

Last 90 days, showing some ongoing, persistent attackers.

Show me the code!

Show me the code!

:-(

Show me the code!

:-)

soon?

Check these out!

- fail2ban = tail log files, filter them, perform actions
- fastnetmon = am I being DDoSed? uses NetFlow/etc
- portsentry = am I being portscanned?
- mod_security + OWASP = Web Application Firewall
- snort = intrusion detection system

Check these out!

- fail2ban = tail log files, filter them, perform actions
- fastnetmon = am I being DDoSed? uses NetFlow/etc
- portsentry = am I being portscanned?
- mod_security + OWASP = Web Application Firewall
- snort = intrusion detection system

- MikroTik MUM London 2016-11-14 (Monday!)

Q?

E: marek@faelix.net
T: @maznu